F

OMPI

SCCR/7/3
ORIGINAL : anglais
DATE : 4 avril 2002

ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE
GENÈVE

COMITE PERMANENT DU DROIT D'AUTEUR ET DES DROITS CONNEXES

Septième session
Genève, 13 – 17 mai 2002

ETUDE SUR LA PROTECTION DES BASES DE DONNEES NON ORIGINALES

Étude établie par M. Sherif El-Kassas,
directeur adjoint du Département d'informatique,
Université américaine du Caire (Égypte)

TABLE DES MATIÈRES[*]

Page

[*] A la demande de ses États membres, l'OMPI a fait réaliser en 2001 cinq études sur l'incidence économique de la protection des bases de données non originales dans les pays en développement et les pays en transition. Les opinions et les résultats des recherches effectuées exposés dans la présente étude n'engagent que la responsabilité de l'auteur de celle-ci et ne doivent pas être considérées comme représentant le point de vue de l'OMPI.

Page

RESUME DE L'ETUDE

La présente étude traite de l'incidence de la protection des bases de données non originales sur les pays en développement. Consacrée exclusivement aux bases de données qui ne sont pas protégées en vertu du droit d'auteur, elle porte essentiellement sur deux aspects principaux : les conséquences éventuelles de la protection des bases de données non originales pour le développement et les solutions techniques proposées en remplacement de la protection juridique.

Dans l'étude, nous donnons un aperçu des principales initiatives visant à protéger les bases de données : le modèle de la Communauté européenne (CE), le modèle proposé par les États-Unis d'Amérique (USA) et des modèles internationaux, et les législations du Mexique et des pays scandinaves. Nous examinons ensuite le pour et le contre de la protection des bases de données non originales. Nous analysons des mesures techniques de protection éventuelles et donnons des exemples d'industries confrontées aux mêmes types de problèmes. Enfin, nous tirons un certain nombre de conclusions. On trouvera dans les appendices du document une présentation plus détaillée de certaines mesures techniques de protection importantes.

Les partisans des initiatives visant à protéger les bases de données affirment que cette protection a notamment pour objectif d'"empêcher que les producteurs de bases de données ne soient menacés par des appropriations préjudiciables au marché de la part de concurrents parasites", [voir 1 dans la bibliographie], de favoriser les investissements dans la collecte de certains types de données et d'assurer un avantage équitable par rapport aux entreprises communautaires (et d'autres régions) qui octroient une protection *sui generis* des bases de données et élargissent cette protection à des entreprises étrangères sous réserve de réciprocité [voir 3 dans la bibliographie].

Toutefois, il est avancé que ce type de protection "aurait [en réalité] pour effet de créer un régime de droits de propriété exclusifs dont la durée serait pratiquement illimitée […]", et qu'il "mettrait en péril la recherche scientifique fondamentale, éliminerait la concurrence sur les marchés en ce qui concerne les produits et services à valeur ajoutée, et transformerait les obstacles actuels à l'admission de ces produits sur les marchés en obstacles juridiques insurmontables".

En conclusion, nous considérons donc que la protection *sui generis* des bases de données non originales, telle qu'elle est proposée actuellement, aurait des répercussions négatives sur les pays en développement et sur les communautés scientifiques et universitaires dans le monde entier. En outre, il est avancé que l'on peut répondre aux préoccupations légitimes de ceux qui sont chargés de compiler les bases de données en recourant soit aux législations et aux mécanismes en vigueur en matière de propriété intellectuelle soit aux mesures techniques visant à protéger leurs systèmes de base de données.

ETUDE

I. AVANT-PROPOS

La présente étude consacrée à l'incidence de la protection des bases de données non originales sur les pays en développement a été réalisée à la demande de l'OMPI. Elle servira au Comité permanent du droit d'auteur et des droits connexes dans le cadre de ses travaux sur la création éventuelle d'un instrument international de protection des bases de données.

La présente étude traite exclusivement des bases de données qui ne sont pas protégées au titre du droit d'auteur (c'est-à-dire celles qui ne satisfont pas au critère d'originalité fixé par la Convention de Berne et par le Traité de l'OMPI sur le droit d'auteur).

Compte tenu de sa formation technique et de son expérience des techniques de l'information dans les pays en développement, de la sécurité des systèmes informatiques et de l'application de ces techniques à la gestion des droits de propriété intellectuelle, l'auteur a axé son étude sur deux principaux thèmes : les incidences éventuelles de la protection des bases de données non originales sur le développement et les mesures techniques proposées en remplacement de la protection juridique.

L'auteur remercie MM. Sherif Saadallah et Shakeel Bhatti de lui avoir apporté leur soutien et de l'avoir orienté vers d'excellents documents de référence.

II. INTRODUCTION

Les partisans des initiatives visant à protéger les bases de données affirment que cette protection a notamment pour objectif "d'empêcher que les producteurs de bases de données ne soient menacés par des appropriations préjudiciables pour le marché de la part de concurrents parasites" [voir 1 dans la bibliographie]; de favoriser les investissements consacrés à la collecte de certains types de données; et enfin de maintenir un avantage équitable par rapport aux entreprises de la Communauté européenne (et d'autres pays) qui octroient une protection *sui generis* des bases de données et qui l'élargissent à des entreprises étrangères sous réserve de réciprocité [voir 3 dans la bibliographie].

Les lois relatives aux bases de données protègent apparemment toute personne qui investit dans la collecte d'éléments d'information et dans la création de bases de données [voir 1 et 6 dans la bibliographie]. Pour bénéficier de cette protection, la base en question ne doit pas nécessairement avoir un contenu original ou constituer en elle-même une œuvre originale.

J.H. Reichmann et P. Samuelson [voir 1 dans la bibliographie] avancent que ce type de protection, telle qu'elle est proposée dans les initiatives de la Communauté européenne et des États-Unis d'Amérique, "aurait pour effet de créer un régime de droits de propriété exclusifs dont la durée serait pratiquement illimitée et qui serait peu, voire nullement, restreint par la politique gouvernementale. Un tel régime mettrait en péril la recherche scientifique fondamentale, éliminerait la concurrence sur les marchés en ce qui concerne les produits et les services à valeur ajoutée, et transformerait les obstacles actuels à l'admission de ces produits et services sur les marchés en obstacles juridiques insurmontables. Les initiatives de la Communauté européenne et des États-Unis d'Amérique pourraient donc aboutir à des prix

relativement élevés pour l'utilisation de biens collectifs. Or, il convient, au contraire, en vertu du principe de l'efficacité économique, d'offrir ce type de biens à des prix très bas et d'appuyer, par des mesures d'encouragement minimales, les investissements et les services requis".

La volonté de protéger juridiquement les bases de données est également motivée par la nature même des systèmes numériques d'information, en raison notamment de la facilité avec laquelle ils permettent d'accéder à des informations publiées en format numérique et de les copier.

Présentation des initiatives relatives à la protection des bases de données[1]

Il est communément admis que le droit d'auteur ne s'applique pas aux bases de données non originales. C'est ce qui explique les efforts déployés pour combler la lacune que présentent la plupart des systèmes de propriété intellectuelle actuels quant à la nécessité de protéger les bases de données. Par conséquent, il a été proposé de protéger "les bases de données ne relevant pas du droit d'auteur au moyen de régimes de propriété intellectuelle ad hoc ou *sui generis* qui diffèrent des modèles classiques du droit d'auteur et du droit des brevets à l'origine des conventions de Paris et de Berne" [voir 1 dans la bibliographie].

a) L'initiative de l'Union européenne

Pour ce qui est de la protection des bases de données, J.H. Reichmann et P. Samuelson [voir 1 dans la bibliographie] indiquent que la Commission et les Communautés européennes poursuivaient un double objectif : 1) harmoniser les règles appliquées par les États membres aux bases de données relevant de la protection au titre du droit d'auteur; et 2) combler la lacune que les régimes de propriété intellectuelle en vigueur semble présenter au sujet des compilations électroniques de données.

La volonté de la Commission européenne d'assurer la protection des bases de données par un droit de propriété exclusif fermement établi a présidé à l'élaboration de la Directive de la CE sur les bases de données [voir 1 dans la bibliographie].

En vertu du droit *sui generis* qui leur est octroyé, les producteurs de bases de données jouissent d'un droit exclusif "d'interdire l'extraction et/ou la réutilisation de la totalité ou d'une partie substantielle, évaluée d'une façon qualitative ou quantitative, du contenu de cette base de données". La durée initiale de ce droit exclusif est d'au moins 15 ans. Le producteur peut sans cesse prolonger cette protection pour une nouvelle période de 15 ans, dès lors qu'il a consacré de nouveaux investissements à sa base de données.

En effet, conformément aux conditions fixées dans la directive de la CE, la protection *sui generis* est accordée "lorsque l'obtention, la vérification ou la présentation [du] contenu atteste un investissement substantiel du point de vue qualitatif ou quantitatif" ou dans le cas de "toute modification substantielle résultant de l'accumulation d'ajouts, de suppressions ou de changements successifs". La directive de la CE ne contient semble-t-il aucune indication

[1] Cette partie se fonde sur l'exposé et les documents cités sous 1 et 6 dans la bibliographie.

concernant l'évaluation du niveau d'investissement requis pour obtenir la protection, lequel reste par conséquent indéterminé. En outre, "il n'y a pas de limite au nombre de modifications, quantitatives ou qualitatives, qui permettent de prolonger la durée de la protection; tout producteur qui investit régulièrement des sommes substantielles pour actualiser, améliorer ou étoffer une base de données existante peut ainsi obtenir une protection perpétuelle" [voir 1 dans la bibliographie].

Il ressort de ce qui précède que le droit *sui generis* dépend exclusivement de *l'investissement*. Toutefois, "l'étendue de la protection accordée, en vertu du texte final de la directive, aux personnes qui investissent dans des bases de données ne relevant pas du droit d'auteur équivaut quasiment désormais à celle octroyée aux créateurs de compilations susceptibles d'être protégées au titre du droit d'auteur" [voir 1 dans la bibliographie].

De plus, conformément à cette directive, "chaque génération indépendante de données, aussi superflue ou banale qu'elle soit, sera protégée pour autant qu'elle coûte de l'argent et sa protection pourra être prolongée indéfiniment dès lors que des dépenses auront été engagées pour réactualiser ou réutiliser ces mêmes données sous forme de mises à jour, d'adjonctions et d'étoffements".

Il s'ensuit que des tiers ne pourront pas éviter les frais nécessaires à la réactualisation de données préexistantes, à moins que le concepteur de la base de données correspondante ne l'ait abandonnée ou n'ait renoncé à exercer ses droits de propriété, comme cela se produit souvent dans le cadre du droit des marques.

De plus, indépendamment du fait qu'il soit possible ou non de réactualiser les données à partir de sources mises à la disposition du public, les personnes ayant investi dans la constitution d'une base de données peuvent toujours refuser à des tiers le droit d'exploiter des données préexistantes dans des applications à valeur ajoutée.

J.H. Reichman et P. Samuelson [voir 1 dans la bibliographie] estiment que, dans la pratique, la directive de la CE ne laisse aucune place à la notion de domaine public. Cela est essentiellement dû au fait qu'à chaque fois que les droits exclusifs d'un producteur d'une base de données sont à nouveau prolongés (en raison de son investissement dans des mises à jour, des adjonctions et des révisions) la base en question est protégée dans son intégralité pour une nouvelle période de 15 ans[2]. Le producteur de la base d'origine est alors plus à même de refuser à des tiers le droit d'élaborer des produits à partir de connaissances scientifiques et techniques préexistantes, d'où un obstacle supplémentaire à l'entrée de ces tiers sur le marché.

Il s'agit là d'un aspect particulièrement important pour les pays en développement et les pays sous-développés qui risquent de ne pas disposer des fonds nécessaires pour se procurer un accès à ces informations. Or, ils pourraient les obtenir gratuitement si elles n'étaient pas protégées.

---

[2] La prolongation de la protection ne se limite pas aux éléments révisés ou ajoutés, comme cela serait le cas dans le cadre des législations sur le droit d'auteur.

b) Modèle américain et modèles internationaux

Les États-Unis d'Amérique et l'Union européenne ont tous deux soumis des propositions en vue d'une protection mondiale des contenus des bases de données dans le cadre de régimes de propriété intellectuelle *sui generis* comparables à celui consacré dans la directive de la CE.

En décembre 1996, l'OMPI a accueilli une conférence diplomatique dans le but d'examiner ces propositions. Le projet de loi et la proposition présentés par les États-Unis d'Amérique prévoient par ailleurs d'étendre la protection aux compilateurs de données. Le compilateur jouirait ainsi des droits exclusifs d'interdire l'extraction et la réutilisation de l'ensemble ou de parties importantes d'une base de données au motif qu'il aurait réalisé des investissements substantiels pour collecter, assembler, vérifier ou présenter les données contenues dans la base. Dans le cas où le compilateur continuerait d'investir dans la mise à jour ou dans l'actualisation de sa base, la durée initiale de protection, à savoir 25 ans, pourrait être continuellement et indéfiniment renouvelée.

En outre, les États-Unis d'Amérique donnent dans leur proposition une définition très large du terme "base de données" en y incluant les composants de programmes informatiques qui ne peuvent pas être protégés au titre du droit d'auteur. Par ailleurs, leur proposition ne prévoit aucune disposition expresse permettant d'exclure certaines informations de la protection, pas même des éléments factuels ou des données compilés aux fins d'ouvrages scientifiques ou historiques. Enfin, toujours conformément à la proposition qu'ils ont soumise à l'OMPI, la durée initiale de la protection accordée aux producteurs de bases de données serait de 25 ans.

La proposition américaine renforce l'aspect le plus dérangeant de la directive de la CE, en ce sens qu'elle ne permet pas la formation d'un domaine public évolutif dans lequel des tiers pourraient venir librement puiser.

"En prévoyant une durée de protection plus longue, des droits exclusifs plus étendus, des sanctions pénales sévères […], et des règles accessoires renforçant la possibilité des producteurs d'appliquer leur propre politique en matière de transmissions en ligne, et enfin en ne reconnaissant pas d'exceptions ni de privilèges d'intérêt public, la loi proposée par les États-Unis d'Amérique revient à placer les détenteurs de bases de données dans une position encore plus monopolistique que celle dont ils bénéficient en vertu de la directive de la CE" [voir 1 dans la bibliographie].

c) Législations nationales

L'OMPI a publié une étude sur la législation nationale de ses États membres [voir 6 dans la bibliographie][3]. Dans le cadre de cette étude, l'OMPI a relevé des dispositions accordant une protection juridique *sui generis* aux bases de données qui ne réunissent pas les critères d'originalité dans les pays suivants : Danemark, Finlande, Islande, Mexique, Norvège et Suède.

[3] Les informations qui ont servi à l'élaboration du reste de cette sous-partie sont tirées du document cité sous 6 dans la bibliographie.

La protection prévue en vertu des lois nordiques (Danemark, Finlande, Islande, Norvège et Suède) s'applique uniquement à la reproduction (en Islande, à la réimpression et à la reproduction) de l'ouvrage en cause. Aucune protection n'est accordée contre d'autres utilisations, et les lois ne précisent pas dans quelle mesure elles sont applicables à l'extraction et à la reproduction non autorisées de parties de compilations protégées.

La durée de la protection et la méthode de calcul utilisée pour la déterminer diffèrent légèrement d'une loi nordique à l'autre. Ainsi, au Danemark, elle est de 10 ans à compter de la fin de l'année au cours de laquelle l'œuvre a été rendue publique, mais ne peut être supérieure à 15 ans après la fin de l'année de sa création; en Finlande, elle est de 10 ans à compter de la fin de la publication de l'ouvrage, mais ne peut être supérieure à 15 ans après la fin de l'année de sa création; en Islande, elle est de 10 ans à compter de la fin de l'année au cours de laquelle l'ouvrage a été publié; en Norvège et en Suède, elle est de 10 ans à compter de la fin de l'année au cours de laquelle l'ouvrage a été publié. Aucune de ces lois ne contient de disposition explicite concernant le renouvellement de cette période lorsque la compilation est, en permanence ou de manière occasionnelle, mise à jour, étoffée ou révisée.

La Loi fédérale sur le droit d'auteur du Mexique prévoit une protection *sui generis* des bases de données en vertu de laquelle la protection est étendue aux bases de données qui ne sont pas originales. Les droits accordés sont des droits exclusifs d'interdire ou d'autoriser les actes suivants : 1) la reproduction permanente ou provisoire, totale ou partielle, par quelque moyen et sous quelque forme que ce soit; 2) la traduction, l'adaptation, la réorganisation et toute autre modification; 3) la distribution de l'original ou des copies de la base de données; 4) la communication publique; et 5) la reproduction, la distribution ou la communication publique des résultats des opérations visées à l'alinéa 2) ci-dessus. Le titulaire initial des droits est la personne qui a fabriqué la base de données. La loi ne comporte aucune disposition explicite concernant le transfert de titularité.

La durée de la protection est de cinq ans. La loi ne comporte aucune disposition explicite concernant le renouvellement de la durée de la protection lorsque la compilation est, en permanence ou de manière occasionnelle, mise à jour, étoffée ou révisée.

III. PROTECTION *SUI GENERIS* DES BASES DE DONNEES : LE POUR ET LE CONTRE[4]

a) Principaux arguments en faveur d'une protection *sui generis* des bases de données

On relève dans le document cité sous 2 dans la bibliographie trois principaux arguments avancés par les partisans de cette protection ainsi que d'autres arguments concernant les pays en développement et les pays sous-développés. Ils peuvent être résumés comme suit :

1. Les investissements considérables que supposent la compilation et la maintenance des bases de données ont besoin d'être davantage protégés, en particulier dans l'environnement numérique en ligne qui facilite la copie des bases de données.

[4] Cette partie s'inspire des documents cités sous 2 et 3 dans la bibliographie.

2. Le droit d'auteur en vigueur ne prévoit aucune protection pour les bases de données globales consultées en ligne au moyen d'un moteur de recherche. Du fait justement de l'exhaustivité de ces bases de données, leur contenu ne résulte pas du choix du compilateur. En outre, la disposition de ces données selon un ordre déterminé n'a lieu que lorsque l'utilisateur effectue une recherche. N'ayant pas fait l'objet d'une sélection ni d'une disposition particulière, ces matières ne peuvent donc pas être protégées au titre du droit d'auteur.

3. La Directive de l'Union européenne procurera aux entreprises communautaires un avantage sur le marché des bases de données. En effet, la directive élargit la protection *sui generis* à des entités non européennes sous réserve de réciprocité et non selon le principe du traitement national. Il en résulte que les entreprises non européennes ne pourront pas bénéficier de la nouvelle protection juridique octroyée aux bases de données en vertu de la directive, à moins que les pays dont elles sont ressortissantes assurent un degré de protection comparable.

4. Dans les pays en développement, la protection peut encourager la constitution de bases de données susceptibles d'avoir des incidences positives sur la croissance de ces pays (du fait que des informations deviennent disponibles grâce à des collections et des compilations). Par ailleurs, les partisans de la protection *sui generis* font valoir qu'elle pourrait contribuer à retenir les investissements étrangers.

b) Principaux arguments contre la protection *sui generis* des bases de données

Un certain nombre d'arguments contre cette forme de protection ont été exposés dans les documents cités sous 2 et 3 dans la bibliographie.

1. Une protection adéquate existe d'ores et déjà dans le cadre de la législation en vigueur sur la propriété intellectuelle. Par exemple, il suffit que les données contenues dans une base fassent l'objet d'une sélection ou d'une disposition minimale pour que la base en question soit protégée au titre des lois sur le droit d'auteur. Certains affirment qu'il s'agit là d'une condition suffisante pour se prémunir contre la copie à grande échelle.

2. Le droit contractuel, les secrets d'affaires et les législations en matière de concurrence déloyale offrent des moyens de protection supplémentaires pour les bases de données que celles-ci relèvent ou non du droit d'auteur.

3. Même sans protection juridique, les compilateurs de bases de données peuvent toujours sauvegarder leurs investissements en recourant à des procédés techniques pour éviter que leur base ne soit copiée. Ces procédés sont examinés plus en détail dans la quatrième partie et dans les appendices de la présente étude.

4. Aucun élément ni aucun exemple concret ne permet de prouver à ce jour qu'un producteur d'une base de données ait renoncé à concevoir un produit par crainte qu'il soit insuffisamment protégé au titre de la propriété intellectuelle. Pour certains, si aucune preuve n'a été produite à ce sujet, c'est qu'aucune n'existe [voir 2 dans la bibliographie].

5. La protection très étendue (prévue dans la proposition des États-Unis d'Amérique) est l'un des points les plus problématiques. Dans la proposition américaine, le terme "base de données" désigne aussi une collection d'ouvrages, de données ou d'autres éléments et correspond donc à une définition globale qui va au-delà de la signification habituellement attribuée à ce terme.

6. La durée de la protection est, elle aussi, problématique. Elle est de 15 ans aux termes de la directive de l'UE, et de 25 ans aux termes de la proposition américaine. Dans tous les cas, ces deux modèles auraient pour effet d'accorder à de nombreuses bases de données une protection perpétuelle, étant donné que toute modification ou actualisation substantielle d'une base de données aboutirait à la création d'une nouvelle base assortie d'une nouvelle période de protection. Cette protection perpétuelle, lorsqu'elle peut s'appliquer à des œuvres actuellement couvertes par le droit d'auteur, a peut-être permis à des producteurs de bases de données de ne pas tenir compte de la durée de la protection prévue au titre du droit d'auteur, entraînant ainsi une contraction importante du domaine public.

7. Objections émises par des scientifiques et des chercheurs. La plupart des types de travaux de recherche nécessitent l'utilisation d'importants volumes de données, voire pour certains, l'utilisation de bases de données entières. Si les bases de données librement accessibles jusqu'à présent font désormais l'objet d'une protection *sui generis*, le coût de la recherche augmentera inévitablement. De plus, une protection *sui generis* incitera les organismes de recherche à considérer leurs bases de données comme des sources de revenus, ce qui nuira au partage des données scientifiques. Une telle protection augmentera le coût de la recherche qui deviendra, selon toute vraisemblance, plus prohibitif encore pour les pays en développement.

8. Objections émises par des concepteurs de logiciels. Conformément à la proposition américaine, la protection portera aussi sur les bases de données intégrées dans des programmes informatiques. Ainsi, les tables de recherche, les ensembles de commandes et de caractères ainsi que d'autres structures de données et d'autres éléments de programme analogues seraient protégés en tant que bases de données. Cette disposition fera obstacle à la conception de logiciels et en augmentera le coût. Un autre aspect est particulièrement important pour les pays en développement : cette forme de protection pourrait les empêcher de tirer profit de logiciels gratuits provenant de sources librement accessibles.

9. Objections émises par des sociétés exerçant leurs activités sur l'Internet[5]. La définition du terme "base de données" qui figure dans la proposition américaine englobe les tables d'indicatifs et les annuaires d'acheminement nécessaires au fonctionnement de l'Internet. Une protection *sui generis* des bases de données pourrait par conséquent conduire à une concentration de la puissance commerciale sur l'Internet. En outre, la transmission non autorisée d'une base de données pourrait engager la responsabilité, du fait d'autrui, du prestataire de services en ligne qui a fourni, à son insu, les installations matérielles et logicielles ayant permis la transmission en question. Ces conséquences sont à l'origine d'un autre sujet de préoccupation important pour les pays en développement, étant donné que cette situation rendra l'expansion de l'Internet au niveau des communautés locales plus onéreuse et plus difficile.

---

[5] On trouvera des informations plus détaillées sur cette question dans le document cité sous 5 dans la bibliographie.

10. Objections émises par des producteurs de bases de données à valeur ajoutée. Les activités d'un bon nombre d'entreprises consistent à extraire, en toute légalité, des renseignements de bases de données existantes et à les valoriser en leur ajoutant des éléments d'information nouveaux ou en les organisant différemment. Avec un régime de protection *sui generis*, c'est l'ensemble de ce secteur d'activités qui est menacé de disparition.

11. Dans les pays en développement, les sociétés qui prennent l'initiative de constituer des bases de données relatives au patrimoine et aux ressources locales peuvent dans la pratique obtenir un monopole préjudiciable qui se répercutera probablement sur le développement et sur l'accès à l'information.

IV. DES SOLUTIONS TECHNIQUES PROPRES A REMPLACER LA PROTECTION JURIDIQUE

Dans les parties précédentes, nous avons esquissé les principaux aspects de la protection s*ui generis* des bases de données. Selon nous, ce type de protection aura des incidences négatives sur le développement. Il reste important néanmoins de ne pas dénier aux compilateurs de bases de données le droit légitime de protéger leurs investissements. Il est fait valoir que, le plus souvent, un degré de protection supérieur à celui prévu en vertu de droits de propriété intellectuelle plus conventionnels n'est pas nécessaire et que, le cas échéant, des moyens techniques peuvent être mis en place pour assurer une protection complémentaire.

a) Systèmes de protection anti-copie

L'industrie informatique propose de nombreux systèmes anti-copie qui servent essentiellement à protéger divers types de contenus sous forme électronique ou multimédia (par exemple, logiciels, musique, données vidéo et livres). Ces systèmes peuvent intervenir au niveau de l'information ou au niveau du dispositif lui-même et recourir pour ce faire à des applications logicielles ou matérielles. Par exemple, l'industrie du DVD utilise le système dit de cryptage de contenus pour protéger les données enregistrées sur ce support. Il en va de même dans le secteur de la musique où les CD sont conçus de telle sorte qu'ils ne puissent pas être aisément copiés. Dans le domaine de la publication électronique, Adobe (*www.adobe.com*) a mis au point le programme Acrobat qui est devenu la norme en la matière. Concrètement, il s'agit d'un outil permettant de créer des livres électroniques; les éditeurs qui souhaitent protéger le contenu des ouvrages peuvent configurer Acrobat pour restreindre la capacité des utilisateurs de reproduire ou de transmettre leurs exemplaires de livres électroniques. Les producteurs de bases de données peuvent au besoin utiliser ce type de systèmes. Par exemple, le producteur d'un CD contenant un annuaire téléphonique peut y intégrer un des dispositifs anti-copie mentionnés ci-dessus. Il pourra ainsi exercer un contrôle sur l'utilisation de sa base de données, sans pour autant faire de celle-ci un monopole perpétuel. On trouvera dans l'appendice A une synthèse de certains des principaux systèmes directement applicables aux bases de données.

b) Programmes ou dispositifs spéciaux de visualisation

Il existe divers systèmes de cryptage pour protéger différents types de données. Par exemple, l'industrie de la radiodiffusion a depuis longtemps mis en place des systèmes de cryptage (avec plus ou moins de succès) pour contrôler l'accès aux services de télévision à péage. Dans le cadre de ces systèmes, le téléspectateur installe un dispositif spécial qui lui permet de regarder les émissions proposées sur une chaîne payante. En résumé, l'organisme de radiodiffusion peut exercer un contrôle sur la capacité du dispositif d'afficher en clair les émissions de la chaîne payante. Ainsi, il peut protéger ses droits en donnant accès à ses programmes seulement aux téléspectateurs qui en ont payé le prix.

En fait, les secteurs du commerce électronique et des transactions en ligne rencontrent des difficultés qui sont, dans l'ensemble, très comparables à celles que connaît l'industrie des bases de données. Cela est particulièrement vrai pour ce qui est de l'authentification des accès. Des procédés de substitution ont été mis en place dans ces secteurs qui ont besoin de techniques d'authentification efficaces pour s'assurer de l'identité des utilisateurs des systèmes et qui emploient diverses techniques de cryptage (en adoptant des solutions logicielles et matérielles) pour maintenir l'intégrité et la sécurité de leurs systèmes. Les principaux problèmes, les exigences et enfin les moyens techniques de protection du commerce électronique sont brièvement exposés dans l'appendice B. La plupart de ces informations peuvent être directement réutilisées pour la protection des bases de données.

Il est possible en effet de mettre en place des systèmes analogues pour les bases de données en ligne. Le dispositif spécial utilisé pour afficher les données pourrait être conçu sous forme d'une application matérielle ou logicielle (ou d'une application combinant ces deux moyens) et permettrait aux producteurs de bases de données de protéger leurs droits sans avoir à recourir à une protection perpétuelle.

V. CONCLUSIONS

Il semble que la protection *sui generis* des bases de données est née du besoin qu'éprouvent les acteurs de ce secteur de protéger les efforts et les investissements qu'ils consacrent à leurs activités et à leurs produits. Toutefois, selon nous, la protection des bases de données aura des effets négatifs importants sur le développement ainsi que sur la libre circulation des informations au sein de la communauté scientifique.

Pour résumer les principaux problèmes évoqués dans la présente étude, il est à craindre que la protection *sui generis* des bases de données ne :

1. restreigne le domaine public et limite donc sensiblement le volume des informations et des données disponibles gratuitement;

2. crée des monopoles permanents et contre-productifs en autorisant les propriétaires de bases de données à prolonger indéfiniment la période de la protection;

3. nuise à la libre circulation des informations au sein de la communauté scientifique mondiale;

4. entrave l’expansion de l’Internet et de l’industrie du logiciel, étant donné que de nombreux composants de logiciels seront protégés et ne pourront plus par conséquent être utilisés gratuitement; et

5. freine, à plusieurs égards, l’essor des pays en développement et des pays sous-développés.

Certains estiment, en outre, qu’il est possible de répondre aux préoccupations légitimes des compilateurs de bases de données en recourant soit aux législations et aux systèmes juridiques en vigueur en matière de propriété intellectuelle soit à des mesures techniques analogues à celles exposées dans les appendices de la présente étude, ou encore en combinant ces deux solutions.

BIBLIOGRAPHIE

[1] J.H. Reichman and Pamela Samuelson, *Intellectual Property Rights in Data?*, *http://eon.law.harvard.edu/h2o/property/alternatives/reichman.html*

[2] Alan D. Sugarman, *Database Protection--Tilting The Copyright Balance*, *http://www.hyperlaw.com/dbprot1.htm*

[3] Jonathan Band and Jonathan S. Gowdy, *Sui Generis Database Protection: Has Its Time Come?*, D-Lib Magazine, June 1997, *http://www.dlib.org/dlib/june97/06band.html*

[4] Anne Linn, History of Database Protection: Legal Issues of Concern to the Scientific Community, *http://www.codata.org/data_access/linn.html*

[5] Gordon Irlam et autres, commentaires de concepteurs de logiciels au sujet du traité de l'OMPI sur les bases de données, *http://www.base.com/gordoni/thoughts/wipo-db.html*

[6] Législations nationales et régionales en vigueur concernant la propriété intellectuelle en matière de bases de données, réunion d'information sur la propriété intellectuelle en matière de bases de données, Genève, 17-19 septembre 1997, WIPO db/im/2. *http://www.wipo.org/eng/meetings/infdat97/db_im_2.htm*

[7] Réunion d'information sur la propriété intellectuelle en matière de bases de données, Genève, 17-19 septembre 1997, *http://www.wipo.org/eng/meetings/infdat97/*

[8] *http://www.wipo.org/eng/meetings/infdat97/db_im_3.htm*

[9] Ross Anderson, *Security Engineering : A guide to building dependable distributed systems*, Wiley, 2001.

[10] Bruce Schneier, *Applied Cryptography*, 2e édition, Wiley, 1996.

[11] Towards Electronic Commerce in Egypt : A Certificate Authority for Egypt, The Electronic Commerce Committee, The Internet Society of Egypt, CAINET'1998.

APPENDICE A : SYSTEMES DE PROTECTION ANTI-COPIE

D'un point de vue technique, le droit d'auteur et la censure relèvent tous deux du contrôle des accès, lequel consiste à n'accorder l'accès à l'information qu'aux membres de certains groupes [voir 9 dans la bibliographie]. La plupart des systèmes couramment utilisés dans le domaine de la protection anti-copie sont directement applicables à la protection des bases de données.

a) Protection contre la copie de logiciels

Les principaux systèmes de protection des logiciels sont les suivants :

– Protection par le matériel grâce à des clés électroniques affectées aux systèmes. Le logiciel peut être copié, mais sans la clé électronique (dispositif anti-copie et anti-intrusion) il ne peut pas fonctionner.

– Installation de logiciels en employant des méthodes qui rendent toute copie locale impossible. Par exemple, en appliquant une technique de modification des tranches du disque dur, laquelle permet de signaler une tranche déterminée du disque dur comme étant défectueuse; le programme devra alors vérifier cette tranche pour garantir le bon fonctionnement du logiciel.

– La détection du profil de l'équipement du logiciel et des habitudes d'utilisation de son propriétaire peut être, elle aussi, un moyen de déterminer si le logiciel est en train d'être copié ou d'être utilisé par son propriétaire légitime.

b) Protection anti-copie des données audio

La protection au titre du droit d'auteur des données audio est un problème déjà ancien qui remonte à l'invention du magnétophone dans les années 60 [voir 9 dans la bibliographie]. Dans l'environnement numérique de l'Internet, la protection contre la copie des données audio est devenue un sujet de préoccupation important dès lors que le format MP3 de compression audio s'est généralisé. Ce format permet en effet aux utilisateurs de compresser des méga-octets de pistes de disques compacts en des kilo-octets de fichiers MP3 qui peuvent être envoyés via l'Internet. L'industrie de la musique s'est efforcée de rendre la copie difficile en mettant au point d'autres formats audio protégés au titre du droit d'auteur (au moyen du filigranage numérique et autres techniques similaires).

c) Données vidéo et télévision à péage

Des systèmes de protection visant à rendre difficile la copie ou le piratage de contenus vidéo existent déjà depuis longtemps dans le domaine des cassettes vidéo et des magnétoscopes. Certains de ces systèmes interviennent directement au niveau logiciel, c'est-à-dire qu'ils dépendent de la façon dont l'enregistrement a été effectué, tandis que d'autres fonctionnent à partir du magnétoscope lui-même. L'industrie de la télévision à péage protège, elle aussi, depuis longtemps ses contenus vidéo, généralement au moyen de décodeurs permettant de décrypter les émissions télévisuelles reçues. Des améliorations ont

constamment été apportées aux dispositifs de décryptage à mesure que le coût de la technique a baissé. Au début des années 70, on utilisait des dispositifs élémentaires pour obtenir des manipulations simples des signaux télévisuels. Dans les années 80, des systèmes plus sophistiqués (tels que VidéoCrypt et EuroCrypt) ont vu le jour. Ils se composaient généralement de trois éléments : 1) services de gestion des abonnements; 2) décodeur; et 3) carte à puce contenant le type de service auquel étaient abonnés les clients et une grille des programmes.

d) Vidéodisque numérique (DVD)

La norme DVD (Digital Video Disk – *vidéodisque numérique*) prend en charge le système dit de cryptage de contenus (CSS). Une application du système CSS est intégrée dans les lecteurs de DVD pour leur permettre de faire fonctionner le programme de protection anti-copie. Il convient toutefois de faire observer que ce procédé n'est pas particulièrement efficace contre la copie. Il n'en demeure pas moins possible d'utiliser des systèmes de même nature, bien que plus robustes, pour la protection des bases de données.

APPENDICE B : MESURES DE SURETE RELATIVES AU COMMERCE ELECTRONIQUE ET LEUR APPLICATION A LA PROTECTION DES BASES DE DONNEES

Les systèmes de commerce électronique et le secteur des bases de données (en ligne) tendent pour une large part vers les mêmes objectifs, à savoir la protection des investissements et de l'intégrité de leurs systèmes. L'objet du présent appendice est d'attirer l'attention sur un certain nombre des principales techniques utilisées à ces fins[6]. Il est possible de recourir à des moyens analogues pour garantir une protection adéquate des bases de données.

a) Exigences et mesures de sûreté applicables au commerce électronique

La sécurité est fondamentale pour le commerce électronique, en particulier lorsque les transactions sont effectuées sur un réseau ouvert dans lequel les utilisateurs n'ont pas confiance, ce qui est le cas de l'Internet. La présente section donne un aperçu de deux aspects importants de la sécurité : les exigences à respecter et les mesures de sûreté.

i) Exigences à respecter

En général, on peut dénombrer cinq exigences principales en matière de sécurité pour le commerce électronique : 1) authentification de l'entité; 2) intégrité du message; 3) non-réfutation; 4) mécanisme d'audit efficace; et 5) confidentialité.

---

[6] Les informations exposées dans le présent appendice sont tirées de l'exposé et du document cités sous 11 dans la bibliographie.

ii) Authentification de l'entité

Cette exigence est nécessaire pour garantir la fiabilité des transactions électroniques. Elle permet de s'assurer que chaque partie prenante d'une transaction est bien celle qu'elle prétend être. Autrement dit, l'authentification de l'entité sert à prévenir les fraudes qui peuvent survenir du fait d'un imposteur se faisant passer pour un établissement financier ou pour un commerçant agréé.

iii) Intégrité du message

Il est nécessaire de garantir l'intégrité du message afin d'éviter les erreurs susceptibles de se produire en raison des modifications que subit le message au cours de son acheminement. Ces modifications peuvent être dues à des manœuvres frauduleuses ou à une erreur au niveau du système de transmission.

iv) Non-réfutation

Ce terme désigne la capacité des systèmes de fonctionner avec des signatures irréfutables. Autrement dit, dès lors qu'une personne a accepté une transaction, la preuve qu'elle a fournie la met dans l'impossibilité de nier son consentement.

v) Audit efficace

Un mécanisme d'audit efficace doit être disponible dans le cas où il faudrait analyser et régler d'éventuels litiges.

vi) Confidentialité

La confidentialité est une exigence courante pour la plupart des transactions financières, qu'elles soient électroniques ou non. Les systèmes électroniques doivent pouvoir garantir l'anonymat de toutes les parties prenantes d'une transaction ainsi que la confidentialité de son objet.

vii) Mesures et mécanismes de sûreté courants

Pour s'assurer que les exigences susmentionnées en matière de sécurité sont remplies, des mécanismes et des mesures de sûreté doivent être mis en place. Dans l'environnement virtuel des systèmes et des réseaux informatiques, les solutions résident dans le vaste domaine de la cryptographie.

viii) Cryptographie

Ce terme désigne la science qui consiste à créer des systèmes cryptographiques (également dénommés systèmes de chiffrement). Les systèmes cryptographiques sont des

méthodes qui permettent de modifier le message de façon à ce que seules certaines personnes puissent annuler ces modifications et rétablir le message sous sa forme originale. En règle générale, les transformations sont effectuées à l'aide de ce qu'il est convenu d'appeler une *clé*. Il s'agit d'un outil qui est fondamental pour verrouiller et déverrouiller des messages.

ix) Cryptographie à clé publique

Lorsqu'on étudie les systèmes cryptographiques à utiliser pour protéger les communications sur un réseau non sécurisé, tel que l'Internet, on recourt souvent aux systèmes cryptographiques à clé publique. Ce type de système utilise deux clés pour résoudre le problème de l'acheminement des clés sur le réseau. L'une des clés, dénommée la clé publique, sert à verrouiller ou à crypter le message, tandis que l'autre, dénommée la clé privée, sert à le déverrouiller ou encore à le décrypter. Afin d'établir des communications sécurisées en utilisant un tel système, les deux interlocuteurs doivent s'échanger leur clé publique. Une fois les clés échangées, l'expéditeur utilisera la clé publique du destinataire pour verrouiller le message qu'il lui adresse et le destinataire utilisera alors la clé privée correspondante pour déverrouiller le message et récupérer le texte sous sa forme originale.

Les systèmes cryptographiques à clé publique peuvent également être utilisés pour créer des signatures cryptographiques. Une telle signature est en fait un code numérique qui est établi au moyen d'une clé privée à laquelle est associé le message à signer. Les méthodes utilisées pour établir la signature sont conçues de telle sorte que chaque signature correspondant à une clé et à une combinaison de messages données est nécessairement unique. Il est possible en outre de vérifier l'authenticité d'une signature au moyen de la clé publique correspondante.

x) Certificats cryptographiques

La cryptographie à clé publique et les systèmes de signature satisfont à la plupart des exigences en matière de sécurité qui ont été exposées précédemment. Reste le problème de l'authenticité de la clé publique. En effet, le simple fait d'utiliser des systèmes à clé publique ne garantit pas l'identité du détenteur de la clé. Dans un système soumis à aucun contrôle, toute personne peut publier une nouvelle clé publique et prendre une nouvelle identité. Cela reviendrait à autoriser une personne, quelle qu'elle soit, à établir son propre passeport ou permis de conduire. Il s'agit bien évidemment d'une situation inacceptable pour toute application qui, comme le commerce électronique, doit remplir des conditions d'authentification et de non-réfutation.

Pour résoudre ce problème (qui est essentiellement un problème de confiance), les utilisateurs du commerce électronique ne sont pas autorisés à employer n'importe quelle paire de clés publique et privée. Ils doivent au contraire se servir de clés qui ont été certifiées par une tierce partie dont l'intégrité est reconnue de tous et qui est communément appelée un organisme de certification (*Certificate Authority* (CA)).

b) Organismes de certification

L'organisme de certification[7] peut se définir comme étant le fournisseur des authentifications et de l'infrastructure de sécurité qui sont nécessaires pour sécuriser davantage les communications sur l'Internet et pour mieux les adapter au commerce électronique. L'organisme de certification établit et délivre des certificats qui contiennent les renseignements permettant d'identifier avec certitude un utilisateur déterminé. Les renseignements relatifs à l'identité d'une personne ainsi que la clé publique correspondante font l'objet d'un module qui est signé par l'organisme de certification.

Le fait que ce module soit signé par l'organisme de certification permet aux utilisateurs du commerce électronique d'en vérifier la validité. Cela est possible parce que tous les utilisateurs sont réputés connaître l'organisme de certification et lui faire confiance.

Protocoles d'authentification

La plupart des protocoles d'authentification modernes se fondent sur la cryptographie à clé publique et dépendent de l'existence d'un organisme de certification. Un certain nombre de ces protocoles sont utilisés sur l'Internet, que ce soit pour la messagerie sécurisée de type courant ou pour le commerce électronique.

Exemples de protocoles de messagerie sécurisée de type courant :

– Le protocole SSL (Secure Socket Layer) a été initialement mis au point par Netscape. Il peut être utilisé pour toute communication effectuée au moyen du protocole TCP/IP. Le plus souvent, il est employé pour établir des connexions Internet sécurisées entre les navigateurs et les serveurs. Le protocole SSL ainsi que le TLS, une version plus récente, font dorénavant partie des protocoles normalisés de l'Internet.

– Le protocole S/MIME (Secure/Multipurpose Internet Mail Extensions). Comme son nom l'indique, le protocole S/MIME comprend un ensemble de spécifications qui permet aux utilisateurs d'échanger du courrier électronique sur l'Internet en toute sécurité.

[Fin du document]

[7] Ce type d'organismes existent désormais couramment dans le cadre plus élaboré de l'infrastructure à clé publique (ICP).